

MULTIMEDIA



UNIVERSITY

STUDENT ID NO

--	--	--	--	--	--	--	--	--	--

MULTIMEDIA UNIVERSITY

FINAL EXAMINATION

TRIMESTER 1, 2019/2020

TNS3131 – NETWORK SECURITY AND MANAGEMENT

(All sections / Groups)

23 October 2019
2.30 p.m. – 4.30 p.m.
(2 hours)

INSTRUCTIONS TO STUDENTS

1. This Question paper consists of 4 pages **including cover page with 5 questions**.
2. Attempt **ALL questions**. All questions carry equal marks and the distribution of the marks for each question is given.
3. Please print all your answers in the Answer Booklet provided.

QUESTION 1

- a) i) How does *active attack* different from *passive attack*? [1 mark]
 ii) Explain *Masquerade* and *Denial of Service* in active attack. [2 marks]
- b) List **SIX (6)** security services. [3 marks]
- c) Using a diagram, label and describe the security model portraying controlled access to information or resources on a computer system, in the presence of possible opponents. [2 marks]
- d) Given the following table, name the types of cryptanalytic attacks based on the amount of information known to the cryptanalyst. [2 marks]

	Known to Cryptanalyst	Type of Attack
1	• Encryption algorithm • Ciphertext • One or more plaintext-ciphertext pairs formed with the secret key	
2	• Encryption algorithm • Ciphertext	
3	• Encryption algorithm • Ciphertext • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key	
4	• Encryption algorithm • Ciphertext • Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key	

QUESTION 2

- a) Explain the importance of Feistel cipher. List any **FOUR (4)** design elements of Feistel cipher. [3 marks]
- b) Explain avalanche effect in Data Encryption Standard (DES) algorithm. [1 mark]
- c) A typical stream cipher encrypts plaintext one bit or one byte at a time.
 i) Describe **THREE (3)** design considerations for a stream cipher. [3 marks]
 ii) Provide a potential advantage of a stream cipher as compared to block cipher. [1 mark]

Continued

- d) Define **TWO (2)** criteria to be met if the encryption scheme is said to be computationally secure. [2 marks]

QUESTION 3

- a) List **SIX (6)** sequences of message exchange in Kerberos V4 and V5. [3 marks]
- b) Illustrate the format of X.509 certificate. [3 marks]
- c) Compare link encryption and end-to-end encryption. [2 marks]
- d) Given binary input data 00110011 01011100 01010010, identify the character representation for Radix-64 encoding (Refer appendix for Radix-64 table). [2 marks]

QUESTION 4

- a) Define S/MIME. Identify **FIVE (5)** S/MIME messages. [3 marks]
- b) Briefly describe **FOUR (4)** potential applications of IP security for secured communication across LAN, WAN and Internet. [2 marks]
- c) In IPSec, explain **TWO (2)** features provided by Authentication Header (AH). [2 marks]
- d) i) Define Secure Electronic Transactions (SET). [1 mark]
ii) Illustrate how SET works. [2 marks]

QUESTION 5

- a) Explain *salt* and list **THREE (3)** purposes of salt in the context of UNIX password management. [3 marks]
- b) Describe **FOUR (4)** phases of typical virus or worm operations. [2 marks]
- c) Briefly explain any **THREE (3)** possible security threats for SNMP. [3 marks]
- d) Compare reactive and proactive network management. [2 marks]

Continued

Appendix:

Radix-64 table

6-Bit Value	Character Encoding	6-Bit Value	Character Encoding	6-Bit Value	Character Encoding	6-Bit Value	Character Encoding
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/
						(pad)	=

End of Paper.